

BARBARA BOXER, CALIFORNIA
 BILL NELSON, FLORIDA
 MARIA CANTWELL, WASHINGTON
 MARK PRYOR, ARKANSAS
 CLARE MCCRILL, MISSOURI
 AMY KLOBUCHAR, MINNESOTA
 MARK WARREN, VIRGINIA
 MARK BISHOP, ALABAMA
 RICHARD BLUMENTHAL, CONNECTICUT
 BRIAN SCHWITZ, HAWAII
 EDWARD MARKEY, MASSACHUSETTS
 CORY A. BOOKER, NEW JERSEY

JOHN THUNE, SOUTH DAKOTA
 ROGER F. WICKER, MISSISSIPPI
 ROY BLUNT, MISSOURI
 MARCO RUBIO, FLORIDA
 KELLY AYOTTE, NEW HAMPSHIRE
 DEAN HELDER, NEVADA
 DAN COATS, INDIANA
 TIM SCOTT, SOUTH CAROLINA
 TED CRUZ, TEXAS
 DEB FISCHER, NEBRASKA
 RON JOHNSON, WISCONSIN

ELLEN CONWAY, STAFF DIRECTOR
 DAVID SCHWITERT, REPUBLICAN STAFF DIRECTOR

United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
 AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEB SITE: <http://commerce.senate.gov>

Received & Inspected

MAY 27 2014

FCC Mail Room

May 12, 2014

540

The Honorable Tom Wheeler
 Chairman, Federal Communications Commission
 445 12th Street, S.W.
 Washington, DC 20554

Dear Mr. Chairman:

As of April 8, 2014, Microsoft has stopped providing free support, including service updates to mitigate potential security vulnerabilities, for Windows XP. We are concerned because, according to news sources, despite the security risks of running outdated and unsupported software, an estimated 10 percent of federal government computers are still running Windows XP, leaving agency systems vulnerable to hackers and cybercriminals.¹ While costly custom agreements with Microsoft to provide continued support may be an option for some users, the continued use of Windows XP with or without custom support comes at a hefty price – both for taxpayers and for the security posture of the federal government.

The Chair of the Internet Security and Privacy Advisory Board in March 2012 wrote to then Acting Director of the Office of Management and Budget Jeffrey Zients, expressing concern with the government's reliance on such systems, stating, "[c]ontinuing to use XP after [the end of support on April 8, 2014] will magnify security risks and associated mitigation costs, considerably."² The Board made the recommendation that the government phase out outdated operating systems, which the Board believed "...would have a significant positive impact on the cyber security posture of Federal agencies, and would demonstrate security leadership by example from the government." The President's Council of Advisors on Science and Technology made a similar recommendation in 2013 to phase out unsupported and insecure operating systems, such as Windows XP.³

The Federal Communications Commission Fiscal Year 2013 Federal Information Security Management Act (FISMA) report did not identify the use of any version of Windows XP on any

¹ Craig Timberg & Ellen Nakashima, *Government computers running Windows XP will be vulnerable to hackers after April 8*, WASH. POST, Mar. 16, 2014, http://www.washingtonpost.com/business/technology/government-computers-running-windows-xp-will-be-vulnerable-to-hackers-after-april-8/2014/03/16/9a9c8c7c-a553-11e3-a5fa-55f0c77bf39c_story.html.

² Letter from Daniel Chenok, Chair, ISPAB to Jeffrey Zients, Acting Director, U.S. Office of Management and Budget (Mar. 30, 2012) available at http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab-ltr-to-omb_outdated-os.pdf.

³ PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., REPORT TO THE PRESIDENT IMMEDIATE OPPORTUNITIES FOR STRENGTHENING THE NATION'S CYBERSECURITY (2013).

Commission assets at the time of the report.⁴ Please confirm that the Commission does not currently own or use any systems running on Windows XP. In the event that the Commission does own or use any systems, operated by or on behalf of the federal government, running on an unsupported operating system such as Windows XP, given the likely security risks of continuing to use unsupported operating systems, we ask that you provide answers to the following questions to assure us that the Federal Communications Commission and its bureaus and offices are making every effort to prioritize the security of federal systems and information.

1. For each of the Federal Information Processing Standard Publication 199 categorized impact levels for systems (High, Moderate, and Low), what is the total number of systems running on unsupported operating systems at the Commission (including each bureau, office or sub-component)?
2. The National Institute of Standards and Technology (NIST) recommends as part of the security controls for federal systems that agencies replace unsupported system components and provide "justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs."⁵ If the Commission or any bureau or office is continuing the use of operating systems and software that no longer receive support, what analysis led to that decision and did the organization follow the NIST recommendation for providing justification and documents approval? Who was involved or consulted in this decision making?
3. Does each bureau or office continuing to run unsupported operating systems such as Windows XP have custom support agreements for such systems? If so, please provide documentation of such agreements, including expectations, security requirements, duration, and total dollar amount.
4. Please provide any Commission plans regarding the use of or transition from unsupported operating systems, such as Windows XP, including, the timeline for transition, associated costs of a transition, including a cost-benefit analysis, and an explanation of how the Commission secures systems running unsupported operating systems during the transition to newer operating systems in order to manage any associated risks and vulnerabilities. If, within the past year, the Commission has made a transition from unsupported operating systems, such as Windows XP, please provide similar information regarding that transition.
5. Describe whether resource limitations have hampered efforts by the Commission to phase out unsupported and insecure operating systems, such as Windows XP.

⁴ FED. COMMUNICATIONS COMM'N, FY 2013 ANNUAL FISMA REPORT: CHIEF INFORMATION OFFICER SECTION REPORT, at 3 (2013).

⁵ U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUBLICATION 800-53 SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS, System and Services Acquisition-22 at F-182 (2013).

Thank you for your prompt attention to this matter. We would appreciate receiving your response to this matter by June 6, 2014. If you have any questions, please contact Cheri Pascoe with the Minority Committee staff at (202) 224-1251 or Meeran Ahn with the Majority Committee staff at (202) 224-1300.

Sincerely,

A handwritten signature in blue ink, appearing to read "Jay Rockefeller".

John D. Rockefeller IV
Chairman

A handwritten signature in blue ink, appearing to read "John Thune".

John Thune
Ranking Member

cc: David A. Bray
Chief Information Officer
Federal Communications Commission



OFFICE OF
THE CHAIRMAN

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

June 27, 2014

The Honorable John D. Rockefeller IV
Chairman
Committee on Commerce, Science, and Transportation
United States Senate
Washington, D.C. 20510

The Honorable John Thune
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate
Washington, D.C. 20510

Dear Chairman Rockefeller and Senator Thune:

I am writing in response to your letter on May 12, 2014, regarding information technology systems operated by the Federal Communications Commission (FCC or Commission). The answers to your specific questions are provided below.

1. For each of the Federal Information Processing Standard Publication 199 categorized impact levels for systems (High, Moderate, and Low), what is the total number of systems running on unsupported operating systems at the Commission (including each bureau, office or sub-component)?

Response: At the time of this response, greater than 97% of the FCC's infrastructure is on supported operating systems. For the remaining 3% or less, the FCC has 45 instances of individual machines running Windows XP, of which 15 are supporting components of FIPS 199 "Moderate" impact systems or General Support Systems (GSS) in the Commission. The remaining 30 systems are standalone workstations. Furthermore, the FCC has 14 instances of machines running unsupported versions of Solaris with all of them supporting FIPS 199 "Moderate" impact systems.

2. The National Institute of Standards and Technology (NIST) recommends as part of the security controls for federal systems that agencies replace unsupported system components and provide "justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs." If the Commission or any bureau or office is continuing the use of operating systems and software that no longer receive support, what analysis led to that decision and did the organization follow the NIST recommendation for providing justification and documents approval? Who was involved or consulted in this decision making?

Response: The FCC has modernization projects underway to transition all servers and all workstations away from unsupported operating systems with the exception of six individual workstations. The continued use of discontinued software has been delayed by funding required to modernize the FCC's legacy infrastructure. For the six individual workstations, the FCC is in the progress of evaluating options, with the intention of performing a risk-based assessment for any system that cannot be transitioned by the end of this fiscal year.

For each instance of an unsupported system, the FCC's Office of the Chief Information Officer (CIO) is in contact with the Bureau or Office at the Commission that is relying on the unsupported system. The Office of the CIO maintains a running list of any such systems. With the arrival of the new FCC CIO, the CIO requested that IT staff with each Bureau or Office at the Commission prepare justification and documentation consistent with the NIST recommendation before the end of the fiscal year.

3. Does each bureau or office continuing to run unsupported operating systems such as Windows XP have custom support agreements for such systems? If so, please provide documentation of such agreements, including expectations, security requirements, duration, and total dollar amount.

Response: The Office of the CIO currently does not require a custom support agreement for any of the systems referenced in the response to question one, as IT support for these systems is provided directly through the Office of the CIO staff. With the arrival of the new FCC CIO, the CIO requested that the Office of the CIO work with each Bureau or Office at the Commission to prepare justification and documentation consistent with the NIST recommendation before the end of the fiscal year. It is the goal of the new CIO to focus considerable IT efforts this year and next year on modernizing the FCC's legacy infrastructure, and move away from unsupported software with dispatch.

4. Please provide any Commission plans regarding the use of or transition from unsupported operating systems, such as Windows XP, including, the timeline for transition, associated costs of a transition, including a cost-benefit analysis, and an explanation of how the Commission secures systems running unsupported operating systems during the transition to newer operating systems in order to manage any associated risks and vulnerabilities. If, within the past year, the Commission has made a transition from unsupported operating systems, such as Windows XP, please provide similar information regarding that transition.

Response: The Commission plans to eliminate the use of unsupported operating systems. Specific projects include: (1) the Virtual Desktop Infrastructure (VDI) project – which moved all user desktops to a virtualized Windows 7 system; (2) fiscal year 2014 license modernization efforts which will commence moving legacy FCC licensing systems away from unsupported software; (3) ongoing FCC server replacement project that also will move away from unsupported hardware and operating systems; and (5) the planned fiscal year 2015 application modernization initiative for aging legacy applications. There will be 29 machines running unsupported operating systems replaced by July 1, 2014 and an additional 24 machines running unsupported operating systems by the end of the calendar year, leaving only the aforementioned six individual workstations.

As the transition and removal of computers with unsupported operating systems are integrated in significantly larger environments and projects, the FCC does not have the specific cost for the operating system transition at this time; it would be a significant effort to produce this information. The Commission is requesting an additional \$13.5 million for information technology efforts in fiscal year 2015 with the intention of modernizing its legacy software, hardware, and custom coded applications to more modern, ideally cloud-based solutions leveraging commercially off-the-shelf software wherever possible. This modernization of the FCC is estimated to be a three year effort done in modular phases, focusing first on removing any unsupported operating systems and aging hardware, and then shifting from outdated custom coded applications to newer ones with the ability to provide data readily to the public, FCC partners, and internal FCC users using more modern security and access-based controls.

5. Describe whether resource limitations have hampered efforts by the Commission to phase out unsupported and insecure operating systems, such as Windows XP.

Response: Due to retirements, flat or declining budgets, and other historical hiring priorities, the FCC's Office of the CIO was limited in its ability to recruit new information technology (IT) talent in recent years. This reduction in the IT staffing numbers has led to severe resource limitations that have delayed system redesigns, upgrades, and replacements causing the FCC to continue the use of unsupported operating systems. Necessary plans and funding for IT modernization have also been a limitation in the past.

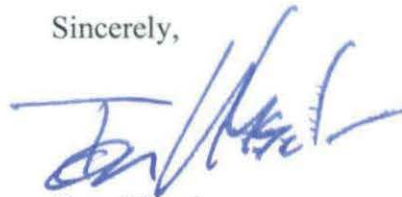
The FCC's fiscal year 2015 budget request to Congress includes initiatives designed to modernize the FCC's information systems. Currently, about 40% of the FCC's application portfolio is more than 10 years old, and 70% of the IT portfolio has a dependency on depreciated legacy technologies. With the arrival of the new FCC CIO,

the Commission is making significant investments in fiscal year 2014 in a modular, modern, open, and standardized computing platform that allows reusability of IT modules across the FCC Bureaus and Offices where appropriate. In fiscal year 2015, the FCC seeks to modernize the application environment using the bottom-up, modular architecture approach to design a current, secure, open-source based, and cloud-friendly framework that is significantly more manageable, sustainable, and consistent with this modern platform. Modular modernization of legacy systems will reduce maintenance and long-term support costs of the portfolio, enable significant application consolidation, improve security controls, enable the Commission to move applications to an external cloud or host, and reduce the risk to critical legacy.

This bottoms-up, modular modernization effort will significantly reduce/enable closure of open FISMA findings, make ongoing remediation efforts more efficient, reduce the risk of cyber exploits on aged infrastructure, and greatly improve the agency's computer security posture. The modular approach will focus on smaller IT modules that can be reused. The modular approach will also incorporate improvements that save time, save money, or reduce the number of personnel required to carry out the work flows of the different FCC Bureaus and Offices. Without this modular modernization effort, FCC legacy application support and maintenance costs will continue to increase at a much higher rate than is sustainable, since support and maintenance for outdated technologies will become more difficult to locate and more costly to procure.

Thank you for your inquiry and allowing us the opportunity to provide you with our current progress and future initiatives. We thank the Committee for their time and effort in working with the FCC on these important topics. Please direct any further questions to Sara W. Morris, Director, Office of Legislative Affairs at 202-418-0095.

Sincerely,

A handwritten signature in blue ink, appearing to read "Tom Wheeler", with a stylized flourish extending to the right.

Tom Wheeler



OFFICE OF
THE CHAIRMAN

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

June 27, 2014

The Honorable John D. Rockefeller IV
Chairman
Committee on Commerce, Science, and Transportation
United States Senate
Washington, D.C. 20510

The Honorable John Thune
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate
Washington, D.C. 20510

Dear Chairman Rockefeller and Senator Thune:

I am writing in response to your letter on May 12, 2014, regarding information technology systems operated by the Federal Communications Commission (FCC or Commission). The answers to your specific questions are provided below.

1. For each of the Federal Information Processing Standard Publication 199 categorized impact levels for systems (High, Moderate, and Low), what is the total number of systems running on unsupported operating systems at the Commission (including each bureau, office or sub-component)?

Response: At the time of this response, greater than 97% of the FCC's infrastructure is on supported operating systems. For the remaining 3% or less, the FCC has 45 instances of individual machines running Windows XP, of which 15 are supporting components of FIPS 199 "Moderate" impact systems or General Support Systems (GSS) in the Commission. The remaining 30 systems are standalone workstations. Furthermore, the FCC has 14 instances of machines running unsupported versions of Solaris with all of them supporting FIPS 199 "Moderate" impact systems.

2. The National Institute of Standards and Technology (NIST) recommends as part of the security controls for federal systems that agencies replace unsupported system components and provide "justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs." If the Commission or any bureau or office is continuing the use of operating systems and software that no longer receive support, what analysis led to that decision and did the organization follow the NIST recommendation for providing justification and documents approval? Who was involved or consulted in this decision making?

Response: The FCC has modernization projects underway to transition all servers and all workstations away from unsupported operating systems with the exception of six individual workstations. The continued use of discontinued software has been delayed by funding required to modernize the FCC's legacy infrastructure. For the six individual workstations, the FCC is in the progress of evaluating options, with the intention of performing a risk-based assessment for any system that cannot be transitioned by the end of this fiscal year.

For each instance of an unsupported system, the FCC's Office of the Chief Information Officer (CIO) is in contact with the Bureau or Office at the Commission that is relying on the unsupported system. The Office of the CIO maintains a running list of any such systems. With the arrival of the new FCC CIO, the CIO requested that IT staff with each Bureau or Office at the Commission prepare justification and documentation consistent with the NIST recommendation before the end of the fiscal year.

3. Does each bureau or office continuing to run unsupported operating systems such as Windows XP have custom support agreements for such systems? If so, please provide documentation of such agreements, including expectations, security requirements, duration, and total dollar amount.

Response: The Office of the CIO currently does not require a custom support agreement for any of the systems referenced in the response to question one, as IT support for these systems is provided directly through the Office of the CIO staff. With the arrival of the new FCC CIO, the CIO requested that the Office of the CIO work with each Bureau or Office at the Commission to prepare justification and documentation consistent with the NIST recommendation before the end of the fiscal year. It is the goal of the new CIO to focus considerable IT efforts this year and next year on modernizing the FCC's legacy infrastructure, and move away from unsupported software with dispatch.

4. Please provide any Commission plans regarding the use of or transition from unsupported operating systems, such as Windows XP, including, the timeline for transition, associated costs of a transition, including a cost-benefit analysis, and an explanation of how the Commission secures systems running unsupported operating systems during the transition to newer operating systems in order to manage any associated risks and vulnerabilities. If, within the past year, the Commission has made a transition from unsupported operating systems, such as Windows XP, please provide similar information regarding that transition.

Response: The Commission plans to eliminate the use of unsupported operating systems. Specific projects include: (1) the Virtual Desktop Infrastructure (VDI) project – which moved all user desktops to a virtualized Windows 7 system; (2) fiscal year 2014 license modernization efforts which will commence moving legacy FCC licensing systems away from unsupported software; (3) ongoing FCC server replacement project that also will move away from unsupported hardware and operating systems; and (5) the planned fiscal year 2015 application modernization initiative for aging legacy applications. There will be 29 machines running unsupported operating systems replaced by July 1, 2014 and an additional 24 machines running unsupported operating systems by the end of the calendar year, leaving only the aforementioned six individual workstations.

As the transition and removal of computers with unsupported operating systems are integrated in significantly larger environments and projects, the FCC does not have the specific cost for the operating system transition at this time; it would be a significant effort to produce this information. The Commission is requesting an additional \$13.5 million for information technology efforts in fiscal year 2015 with the intention of modernizing its legacy software, hardware, and custom coded applications to more modern, ideally cloud-based solutions leveraging commercially off-the-shelf software wherever possible. This modernization of the FCC is estimated to be a three year effort done in modular phases, focusing first on removing any unsupported operating systems and aging hardware, and then shifting from outdated custom coded applications to newer ones with the ability to provide data readily to the public, FCC partners, and internal FCC users using more modern security and access-based controls.

5. Describe whether resource limitations have hampered efforts by the Commission to phase out unsupported and insecure operating systems, such as Windows XP.

Response: Due to retirements, flat or declining budgets, and other historical hiring priorities, the FCC's Office of the CIO was limited in its ability to recruit new information technology (IT) talent in recent years. This reduction in the IT staffing numbers has led to severe resource limitations that have delayed system redesigns, upgrades, and replacements causing the FCC to continue the use of unsupported operating systems. Necessary plans and funding for IT modernization have also been a limitation in the past.

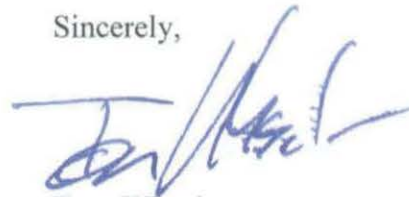
The FCC's fiscal year 2015 budget request to Congress includes initiatives designed to modernize the FCC's information systems. Currently, about 40% of the FCC's application portfolio is more than 10 years old, and 70% of the IT portfolio has a dependency on depreciated legacy technologies. With the arrival of the new FCC CIO,

the Commission is making significant investments in fiscal year 2014 in a modular, modern, open, and standardized computing platform that allows reusability of IT modules across the FCC Bureaus and Offices where appropriate. In fiscal year 2015, the FCC seeks to modernize the application environment using the bottom-up, modular architecture approach to design a current, secure, open-source based, and cloud-friendly framework that is significantly more manageable, sustainable, and consistent with this modern platform. Modular modernization of legacy systems will reduce maintenance and long-term support costs of the portfolio, enable significant application consolidation, improve security controls, enable the Commission to move applications to an external cloud or host, and reduce the risk to critical legacy.

This bottoms-up, modular modernization effort will significantly reduce/enable closure of open FISMA findings, make ongoing remediation efforts more efficient, reduce the risk of cyber exploits on aged infrastructure, and greatly improve the agency's computer security posture. The modular approach will focus on smaller IT modules that can be reused. The modular approach will also incorporate improvements that save time, save money, or reduce the number of personnel required to carry out the work flows of the different FCC Bureaus and Offices. Without this modular modernization effort, FCC legacy application support and maintenance costs will continue to increase at a much higher rate than is sustainable, since support and maintenance for outdated technologies will become more difficult to locate and more costly to procure.

Thank you for your inquiry and allowing us the opportunity to provide you with our current progress and future initiatives. We thank the Committee for their time and effort in working with the FCC on these important topics. Please direct any further questions to Sara W. Morris, Director, Office of Legislative Affairs at 202-418-0095.

Sincerely,

A handwritten signature in blue ink, appearing to read "Tom Wheeler", with a stylized flourish at the end.

Tom Wheeler